

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

GOOGLE LLC,

Plaintiff,

v.

Civil Action No. 1:21-cv-10260-DLC

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
Does 1-15,

Defendants.

**MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR
DEFAULT JUDGMENT AND PERMANENT INJUNCTION**

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

BACKGROUND 2

 I. The Glupteba Botnet..... 2

 II. Service On the Doe Defendants 3

LEGAL STANDARD..... 5

ARGUMENT 6

 I. Google Has Established Jurisdiction And Liability Against The Doe Defendants..... 6

 II. Google Is Entitled To A Permanent Injunction. 9

CONCLUSION..... 12

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Am. Freedom Def. Initiative v. Metro. Transp. Auth.</i> , 889 F. Supp. 2d 606 (S.D.N.Y. 2012)	9
<i>Amusement Indus., Inc. v. Stern</i> , 2016 WL 7016855 (S.D.N.Y. Nov. 30, 2016)	8
<i>Antetokounmpo v. Searcy</i> , 2021 WL 3233417 (S.D.N.Y. May 20, 2021)	5, 6
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	6
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007)	6
<i>BMaddox Enterprises LLC v. Milad Oskouie, Osko M Ltd.</i> , 2021 WL 3675072 (S.D.N.Y. Aug. 18, 2021)	9
<i>Church of Scientology Int’l v. Elmira Mission of Church of Scientology</i> , 794 F.2d 38 (2d Cir. 1986)	10
<i>City of New York v. Mickalis Pawn Shop, LLC</i> , 645 F.3d 114 (2d Cir. 2011)	8
<i>Display Techs., LLC v. Leantegra, Inc.</i> , 2022 WL 354667 (S.D.N.Y. Feb. 7, 2022)	6
<i>FTC v. Verity Int’l, Ltd.</i> , 2000 WL 1805688 (S.D.N.Y. Dec. 8, 2000)	11
<i>FXDirectDealer, LLC v. Abadi</i> , 2012 WL 1155139 (S.D.N.Y. Apr. 5, 2012)	11
<i>Khepera-Bey v. Santander Consumer USA, Inc.</i> , 2013 WL 3199746 (D. Md. June 21, 2013)	10
<i>Licci v. Lebanese Canadian Bank</i> , 732 F.3d 161 (2d Cir. 2013)	6

<i>Mason Tenders Dist. Council Welfare Fund v. Shelbourne Constr. Corp.</i> , 2020 WL 7028530 (S.D.N.Y. Nov. 30, 2020)	5
<i>Microsoft Corp. v. Does 1–8</i> , 2015 WL 4937441 (E.D. Va. Aug. 17, 2015)	11
<i>New York C.L. Union v. New York City Transit Auth.</i> , 684 F.3d 286 (2d Cir. 2012)	9
<i>Rovio Entm't, Ltd. v. Allstar Vending, Inc.</i> , 97 F. Supp. 3d 536 (S.D.N.Y. 2015)	9
<i>Schwab Short-Term Bond Mkt. Fund v. Lloyds Banking Grp. PLC</i> , 22 F.4th 103 (2d Cir. 2021)	7
<i>Tambriz v. Taste & Sabor LLC</i> , 2021 WL 6754956 (S.D.N.Y. December 29, 2021)	6
<i>US Airways, Inc. v. US Airline Pilots Ass'n</i> , 813 F. Supp. 2d 710 (W.D.N.C. 2011)	11
<i>World Wide Polymers, Inc. v. Shinkong Synthetic Fibers Corp.</i> , 694 F.3d 155 (2d Cir. 2012)	9
Statutes	
15 U.S.C. § 1116(a)	11
18 U.S.C. § 1965	7
28 U.S.C. § 1367	7
28 U.S.C. § 1391(b)	7
28 U.S.C. § 1391(c)	7
28 U.S.C. § 1331	7
ECPA	7, 8, 11
Lanham Act	7, 8, 11
RICO	7, 8
Other Authorities	
Federal Rule of Civil Procedure 55	5

Rule 4(f)(3)	3
Rule 55(b)	5

Plaintiff Google LLC (“Google”) seeks a default judgment and permanent injunction against Defendants John Does 1–15 (the “Doe Defendants”) to prevent the Doe Defendants from continuing to operate the malicious computer network and cybercriminal operation known as “Glupteba.”

PRELIMINARY STATEMENT

As set forth in previous pleadings and the Court’s previous orders, the Glupteba Enterprise is a cybercriminal operation engaged in various illicit schemes. The Doe Defendants, as members of the Enterprise and participants in its various schemes, use malware to steal account credentials, commit credit card fraud, mine cryptocurrency, and threaten denial-of-service attacks. Through these actions and others, the Doe Defendants have caused, and continue to cause, harm to Google, its customers, and the public.

Google has made every attempt to serve the Doe Defendants. In addition to publishing the Complaint and other relevant documents on a publicly available website, Google served the materials to fifty email addresses, phone numbers (by text message), and WhatsApp accounts. It appears forty of those various accounts received those messages. Nevertheless, none of the recipients of those messages have responded to the Complaint. Default judgment is therefore warranted.

This Court should also grant Google’s request for a permanent injunction consistent with this Court’s preliminary injunction (ECF No. 17). The Enterprise’s continued and ongoing attempts to reconstitute the Enterprise demonstrate that permanent injunctive relief is both appropriate and needed.

BACKGROUND

As this Court is familiar with the factual and procedural history of the case, Google will recount only the relevant background sufficient to provide context for this motion.¹

I. The Glupteba Botnet

Doe Defendants have deployed the Glupteba malware to form a botnet—a network of internet-connected devices, each of which is infected by the Glupteba malware. *See* Huntley Decl. ¶¶ 13-15 (ECF No. 21). This malware has silently infiltrated more than a million computers and other devices around the globe and is used by the Enterprise for a variety of illicit purposes. *Id.* ¶¶ 15-17. It is used to steal personal login information in connection with the Stolen Accounts Scheme; to facilitate the use of unfunded credit cards to purchase ads (“Credit Card Fraud Scheme”); to sell disruptive ads to display on infected devices (“Disruptive Ad Scheme”); to sell access to infected devices to relay, or “proxy,” communications (“Proxy Scheme”); and to hijack computing power of infected devices to generate cryptocurrency (“Cryptojacking Scheme”). *Id.* ¶¶ 43-77.

To execute these schemes, the Enterprise has used various public facing websites (or “storefronts”) to, for example, sell access to stolen accounts or IP

¹ Additional factual background is set forth in Google’s Complaint (ECF No. 5), its request for a temporary restraining order (ECF No. 9), the Huntley Declaration (ECF No. 21), and the Bisbee Declaration (ECF No. 22).

addresses for use as proxies (dont.farm and AWMProxy.net), and to recruit developers (Voltronwork.com and Undefined.team). *Id.* ¶¶ 45–55, 65–73, 82–85.

The Doe Defendants are unnamed co-conspirators whose true identities are not ascertainable despite Google’s diligent attempts to identify all defendants responsible for the Enterprise’s criminal schemes. Declaration of Laura Harris (“Harris Decl.”) ¶ 3. Each of the Doe Defendants is responsible in some manner for the conduct detailed in Google’s allegations, and each has agreed to become part of the Enterprise. *See id.*; Complaint ¶¶ 18, 111 (ECF No. 5).

II. Service On the Doe Defendants

Pursuant to Rule 4(f)(3), this Court authorized service of the Doe Defendants by internet publication, email, and text message. *See* ECF No. 65. Google effectuated service on the Doe Defendants by these means.

As this Court knows, Google has worked to disrupt the botnet by serving the Court’s Temporary Restraining Order (“TRO”) and Preliminary Injunction Order on relevant domain registrars and other entities. In connection with that process, many of those entities provided contact information for the accounts used to register domains associated with the Enterprise—including email addresses and phone numbers. Harris Decl. ¶ 12. Google used that contact information to serve the Does.

Service By Publication. Google created the publicly available website: <https://www.serviceofprocess.xyz/glupteba>. *Id.* ¶ 16, Ex. 5. The website contains a description of the lawsuit, along with the instruction: “You must ‘appear’ in this case or the other side will win automatically. To ‘appear’ you must file with the court a legal document called a ‘motion’ or ‘answer.’” *Id.* ¶ 17, Ex. 5.

The website also contains links to all the relevant pleadings and orders, as well as contact information for Google’s counsel. *Id.* ¶ 16, Ex. 5. The available documents include the Complaint, the Summonses, the TRO, the Preliminary Injunction Order, the order permitting service on the Doe Defendants, and numerous other filings.

Service By Email. In connection with its botnet disruption efforts, Google obtained 20 email addresses used to register domains associated with the Enterprise. *Id.* ¶ 19-20. Google’s counsel sent an email to each of these addresses on May 13, 2022. *Id.* ¶ 21. Each email stated:

A lawsuit has been initiated against you in the United States District Court for the Southern District of New York. The following link contains copies of the restraining order, summons and complaint, and related filings.

<https://www.serviceofprocess.xyz/glupteba>

Regards,
King & Spalding LLP

Id. ¶ 20. Delivery failure notifications were received for only five of the twenty emails sent. *Id.* ¶ 22.

Service By Text Message. In connection with its botnet disruption efforts, Google also obtained twenty-six phone numbers used to register domains associated with the Enterprise. *Id.* ¶ 23. Google’s counsel sent a text message to each of these phone numbers on May 13, 2022. *Id.* ¶ 23-25. The content of the text messages was identical to the email described above. Only four of the twenty-six messages returned delivery failure notifications. *Id.* ¶ 24. In other words, twenty-two text messages were successfully delivered (inclusive of the WhatsApp messages below). *Id.*

Service By WhatsApp. Of the twenty-six phone numbers, four had WhatsApp accounts. *Id.* ¶ 25. Google’s counsel sent a WhatsApp message to each of these phone numbers on May 13, 2022. *Id.* Three of those four WhatsApp accounts opened the message that was sent to them. *Id.*

* * *

To date, Google has not received any response to any of its attempts at service. *Id.* ¶¶ 1, 21. Nor have any new defendants appeared before this Court. Accordingly, pursuant to Google’s request, the Clerk of Court entered a Certificate of Default as to the Does. ECF No. 85.

LEGAL STANDARD

“Federal Rule of Civil Procedure 55 sets out a two-step procedure to be followed for the entry of judgment against a party who fails to defend: the entry of a default, and the entry of a default judgment.” *Mason Tenders Dist. Council Welfare Fund v. Shelbourne Constr. Corp.*, 2020 WL 7028530, at *2 (S.D.N.Y. Nov. 30, 2020) (citing *New York v. Green*, 420 F.3d 99, 104 (2d Cir. 2005)).

“The first step, entry of a default, ‘formalizes a judicial recognition that a defendant has, through its failure to defend the action, admitted liability to the plaintiff.’” *Id.* (quoting *City of New York v. Mickalis Pawn Shop, LLC*, 645 F.3d 114, 128 (2d Cir. 2011)). Second, “[o]nce the Clerk issues a certificate of default, the moving party may apply for entry of default judgment, pursuant to Rule 55(b).” *Antetokounmpo v. Searcy*, 2021 WL 3233417, at *2 (S.D.N.Y. May 20, 2021), *adopted by* 2021 WL 3233005 (June 23, 2021).

The entry of “default constitutes an admission of all well-pleaded factual allegations in the complaint, and the allegations as they pertain to liability are deemed true.” *Id.* “Whether entry of default judgment at the second step is appropriate depends upon whether the well-pleaded allegations against the defaulting party establish liability as a matter of law.” *Display Techs., LLC v. Leantegra, Inc.*, 2022 WL 354667, at *2 (S.D.N.Y. Feb. 7, 2022) (citing *Mickalis Pawn Shop*, 645 F.3d at 137).

“The legal sufficiency of a non-defaulting party’s claims ‘is analyzed under the familiar plausibility standard enunciated in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), aided by the additional step of drawing inferences in the movant’s favor.” *Id.* (citation omitted). “The court may also rely on factual allegations pertaining to liability contained in affidavits and declarations submitted by the plaintiff.” *Tambriz v. Taste & Sabor LLC*, 2021 WL 6754956, at *7 (S.D.N.Y. December 29, 2021).

ARGUMENT

I. Google Has Established Jurisdiction And Liability Against The Doe Defendants.

As the Court has previously found, jurisdiction is proper, venue is proper, and Google has stated a claim. ECF No. 5, ¶¶ 1, 2, 4, 8-13; ECF No. 62 at 24.

Personal Jurisdiction. “Determining personal jurisdiction over a foreign defendant in a federal-question case such as this requires a two-step inquiry.” *Licci v. Lebanese Canadian Bank*, 732 F.3d 161, 168 (2d Cir. 2013). First, the court must find that jurisdiction lies under New York’s long-arm statute. *Id.* “If jurisdiction lies,”

then the court must find that its “exercise of personal jurisdiction over a foreign defendant comports with due process protections established under the United States Constitution.” *Id.*

As the Court has already found, Google’s allegations that “defendants operate a botnet that has infected over one million devices, at least thousands of which are located in New York City,” and “intentionally infected devices in New York in order to steal victims’ personal information” are sufficient “to establish personal jurisdiction under New York’s long arm statute and the Due Process Clause.” ECF No. 62 at 14; *see also Schwab Short-Term Bond Mkt. Fund v. Lloyds Banking Grp. PLC*, 22 F.4th 103, 123 (2d Cir. 2021) (defendants subject to personal jurisdiction where “a co-conspirator’s overt acts in furtherance of the conspiracy had sufficient contacts with a forum to subject that co-conspirator to jurisdiction in that forum”) (brackets omitted).

Subject Matter Jurisdiction. Pursuant to 28 U.S.C. § 1331, the Court has federal-question jurisdiction under over Google’s claims under RICO, the CFAA, the ECPA, and the Lanham Act. The Court has supplemental jurisdiction over Google’s state-law claims for tortious interference with a business relationship and unjust enrichment under 28 U.S.C. § 1367.

Venue. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because the Doe Defendants are not residents of the United States and may be sued in any judicial district. *See* ECF No. 5, ¶¶ 16-18, 21. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial

part of the events or omissions giving rise to Google’s claims occurred in this judicial district; because a substantial part of the property that is the subject of Google’s claims is situated in this judicial district; because a substantial part of the harm caused by the Doe Defendants has occurred in this judicial district; and because the Doe Defendants transact their affairs in this judicial district. *See* ECF No. 5, ¶ 20; ECF No. 10, ¶ 92.

Liability. “When determining the liability of a party in default, a court must accept the factual allegations of the party moving for default judgment as true, and draw all reasonable inferences in its favor.” *Amusement Indus., Inc. v. Stern*, 2016 WL 7016855, at *2 (S.D.N.Y. Nov. 30, 2016) (citing *Finkel v. Romanowicz*, 577 F.3d 79, 84 (2d Cir. 2009)). A plaintiff is entitled to default judgment if its complaint states a claim upon which relief can be granted. *Mickalis Pawn Shop*, 645 F.3d at 137.

The Court has previously found that the Complaint “pleads facts with the specificity required by the Federal Rules and states claims against Defendants for violations” of the CFAA, the ECPA, the Lanham Act, and RICO, and for tortious interference with business relationship and unjust enrichment under New York common law. ECF No. 5, ¶¶ 4, 8-13; ECF No. 62 at 24. The Doe Defendants’ default therefore establishes their liability on each of Google’s causes of action. *See Amusement Indus. v. Stern*, 2016 WL 7016855, at *2 (S.D.N.Y. Nov. 30, 2016) (“In this case, the Court has already held that plaintiffs’ third amended complaint states

a claim against FRG Corp. Accordingly, FRG Corp.’s default establishes its liability on the four causes of action that the Court found stated a claim.”) (citations omitted).²

II. Google Is Entitled To A Permanent Injunction.

“It is well established that a court may grant a permanent injunction as part of a default judgment.” *BMaddox Enterprises LLC v. Milad Oskowie, Osko M Ltd.*, 2021 WL 3675072, at *15 (S.D.N.Y. Aug. 18, 2021); *see Rovio Entm’t, Ltd. v. Allstar Vending, Inc.*, 97 F. Supp. 3d 536, 546 (S.D.N.Y. 2015) (collecting cases).

As noted above, the Court has already granted a TRO and a preliminary injunction, the latter of which remains in effect. *See* ECF No. 9. “The requirements for a permanent injunction are ‘essentially the same’ as for a preliminary injunction, except that the moving party must demonstrate ‘actual success’ on the merits.” *New York C.L. Union v. New York City Transit Auth.*, 684 F.3d 286, 294 (2d Cir. 2012); *Am. Freedom Def. Initiative v. Metro. Transp. Auth.*, 889 F. Supp. 2d 606, 611 (S.D.N.Y. 2012) (similar). Because Google has now established liability conclusively, as shown above, it is entitled to a permanent injunction.

Further, to secure a permanent injunction, a plaintiff must demonstrate that: (1) it has suffered an irreparable injury; (2) remedies available at law are inadequate to compensate for that injury; (3) in light of the hardships on the plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *World Wide Polymers, Inc. v. Shinkong*

² Google has previously set forth additional detail regarding the bases for Defendants’ liability for each of Google’s claims. *See* ECF No. 51 at 14–17; ECF No. 19 at 9–18; *see generally* ECF Nos. 11, 22.

Synthetic Fibers Corp., 694 F.3d 155, 160–161 (2d Cir. 2012) (citing *eBay Inc. v. MercExchange LLC*, 547 U.S. 388, 391 (2006)).

Irreparable Injury And Inadequate Remedies At Law. Google has established that it was irreparably injured and that legal remedies are inadequate to compensate for that harm. Circumstances “such as insolvency or satisfiability of a money judgment, can show irreparable harm.” *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 WL 3199746, at *4 (D. Md. June 21, 2013). The Enterprise has already infected one million devices with malware.

Google has employed technical measures to protect itself from the harm to its systems caused by this malware, but those actions come at a cost. It has already spent more than 2,000 hours, and well in excess of \$100,000, investigating the Glupteba botnet and seeking to protect Google and its users from the Enterprise’s misconduct. ECF No. 10, ¶ 95. That harm is unlikely to ever be compensated—even after final judgment—because the Enterprise is controlled by elusive cybercriminals who will take steps to avoid complying with any judgment. Without continued injunctive relief to prevent its reconstitution, the Enterprise will continue to infect thousands of new devices, conscripting those machines into tools for its cybercrimes. *See* ECF No. 5, ¶ 29; ECF No. 10, ¶¶ 4, 90.

In addition, the Doe Defendants’ conduct is tarnishing Google’s valuable trademarks, injuring Google’s goodwill, and damaging its reputation by creating confusion as to the source of the Glupteba malware and false messages. Consumer confusion and injury to business goodwill constitute irreparable harm. *E.g., Church*

of *Scientology Int'l v. Elmira Mission of Church of Scientology*, 794 F.2d 38, 44 (2d Cir. 1986) (loss to “reputational value and goodwill” are irreparable harm); *Microsoft Corp. v. Does 1–8*, 2015 WL 4937441, at *10 (E.D. Va. Aug. 17, 2015) (“[T]he surreptitious nature of the Shylock botnet is damaging to the Plaintiffs’ brands and the customer goodwill engendered by their products and trademarks.”). Moreover, Google is entitled to a presumption of irreparable harm upon a showing, as Google makes here, of its meritorious Lanham Act claims. *See* 15 U.S.C. § 1116(a).

Balance Of Hardships. The equities also favor a permanent injunction. The Doe Defendants, through their participation in the Enterprise, defraud consumers and injure Google. There is no countervailing weight. There is no legitimate reason why the Doe Defendants should be permitted to continue to disseminate malware and control infected computers. *See, e.g., FTC v. Verity Int’l, Ltd.*, 2000 WL 1805688, at *1 (S.D.N.Y. Dec. 8, 2000) (balance of equities weighs in favor of injunctive relief where defendant’s practices violate a federal statute); *US Airways, Inc. v. US Airline Pilots Ass’n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (same).

Public Interest. Finally, a permanent injunction would serve the public interest. Prior to this Court’s injunctive relief, as many as 60,000 devices became infected with Glupteba malware in a single day. The public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA, the ECPA, and Lanham Act. *See, e.g., FXDirectDealer, LLC v. Abadi*, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (“[T]he public has an interest in seeing that . . . cyber-fraud is prevented.”).

The Court's preliminary injunctive, therefore, should become permanent.

CONCLUSION

For the forgoing reasons, this Court should enter default judgment for Google and issue a permanent injunction against the Doe Defendants.

DATED: July 19, 2022

Respectfully submitted,

/s/ Laura Harris

Laura Harris
Andrew Michaelson
Kathleen E. McCarthy
Matthew Bush
KING & SPALDING LLP
1185 Avenue of the Americas,
34th Floor
New York, NY 10036
Telephone: (212) 790-5356
Fax: (212) 556-2222
lharris@kslaw.com
amichaelson@kslaw.com
kmccarthy@kslaw.com
mbush@kslaw.com

Sumon Dantiki (*pro hac vice*)
David P. Mattern (*pro hac vice*)
KING & SPALDING LLP
1700 Pennsylvania Ave., NW,
2nd Floor
Washington, DC 20006
Telephone: (202) 626-5591
Fax: (202) 626-3737
sdantiki@kslaw.com
dmattern@kslaw.com

Counsel for Plaintiff Google LLC